# Footprinting e Ingeniería Social

## Agenda

- Definición de Footprinting
- Metodología de recopilación de información
- Inteligencia competitiva
- Enumeración de DNS
- Whois y ARIN Lookups
- Identificación de los tipos de registros DNS
- Traceroute en el Footprinting
- E-Mail Tracking
- Web Spiders
- ¿Qué es la Ingeniería Social?
- Comportamientos vulnerables a ataques
- Fases de la Ingeniería SocialTipos de ataques comunes



## Agenda (Cont.)

- Comprendiendo los ataques internos
- Comprendiendo el robo de identidad
- Ataques de Phishing
- Online Scams
- Ofuscación de URLs
- Contramedidas

## Definición de Footprinting

- Footprinting es el proceso de creación de un mapa de las redes y sistemas de una organización.
- Está incluido en el proceso de "recopilación de información" (Information Gathering).
- El Footprinting comienza por la determinación del target, para luego averiguar información específica utilizando métodos no intrusivos.
- Una herramienta fundamental son las búsquedas online, utilizando Google u otro buscador. Es importante conocer en profundidad las características avanzadas de búsqueda (site:, intitle:, allinurl:, etc.)



## Definición de Footprinting (Cont.)

- Junto al escaneo y enumeración, el footprinting es una de las tres fases de obtención de información antes de un ataque.
- Un atacante suele utilizar el 90% de su tiempo en las primeras etapas.
- El footprinting resultará en un único perfil en la red para cada organización.



## Metodología de Recopilación de Información

- La obtención de información sobre un objetivo se realiza antes de un ataque.
- La metodología utilizada considera tres etapas: *Footprinting*, *Scanning* y *Enumeration*.
- De manera general puede ser dividida en siete pasos.
  - Detectar la información inicial
  - Ubicación del rango de red
  - Comprobación de equipos activos
  - Descubrimiento de puertos abiertos y puntos de acceso
  - Detección del sistema operativo
  - Descubrimiento de servicios en los puertos
  - Mapeo de red
- El proceso de footprinting se realiza durante los primeros dos pasos.

## Metodología de Recopilación de Información (Cont.)

- Algunas fuentes comunes de información incluyen el uso de:
  - Domain name lookup
  - Whois
  - Nslookup
- La mayor parte de la información puede obtenerse libremente y de manera legal.
- Es muy importante comprender el sistema de resolución de nombres de dominio (DNS) para lograr una profunda comprensión de esta etapa y del funcionamiento de Internet.



## Inteligencia Competitiva

- Implica la averiguación de información sobre la competencia (productos, tecnologías, marketing, etc.)
- Existen diversas herramientas que pueden ser utilizadas para esto.
- La inteligencia competitiva incluye diversos temas como ser:
  - Recopilación de datos
  - Análisis de datos
  - Verificación de información
  - Seguridad de la información
- Existen muchas empresas privadas que ofrecen el servicio de inteligencia competitiva



## Búsqueda de Información en Internet

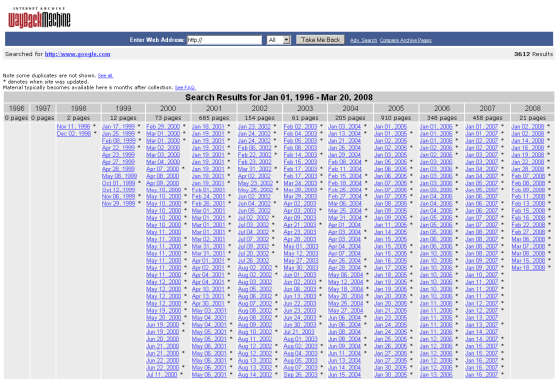
- Buscando en Internet la dirección de correo electrónico o el nombre de una persona podemos encontrar en las listas de correo, foros, etc. información sobre la empresa donde trabaja.
- Otra fuente de información útil son las redes sociales y los sitios de empleos.

## Archivo Histórico: http://www.archive.org

- Esta iniciativa guarda la mayor parte de los sitios web de Internet y alberga obras culturales de dominio público o con licencias abiertas.
- Se dedica desde 1996 a recoger sistemáticamente copias de los sitios web de todo el mundo, permitiendo estudiar su evolución.
- La herramienta que permite consultar sitios históricos se denomina: *Wayback Machine*




## Archivo histórico: htto://www.archive.org (Cont.)




## Enumeración de DNS

- El sistema de resolución de nombres permite básicamente transformar nombres de dominio en direcciones IP.
- Le corresponden los RFC 1034 y 1035
- La enumeración de DNS es el proceso de ubicación de todos los servidores DNS y sus correspondientes registros de una organización.
- Una compañía puede tener DNS internos y externos que pueden brindar diferentes datos del objetivo.

## Enumeración de DNS (Cont.)

- El sistema DNS utiliza tres componentes principales
  - Clientes DNS
  - Servidores DNS
  - Zonas de autoridad
- El DNS consiste en un conjunto jerárquico de servidores DNS.
- Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio.
- La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentra los servidores raíz, que responden cuando se busca resolver un dominio de primer y segundo nivel.



## Enumeración de DNS (Cont.)

- Es posible utilizar herramientas varias y sitios web especializados para realizar esta etapa de enumeración de DNS.
- Tal vez la herramienta elemental para enumeración de DNS sea NSLookup, disponible en todos los sistemas operativos.
- Durante el año 2008 se encontraron diversas vulnerabilidades al sistema de DNS y a una de las herramientas de NSLookup mas difundidas. Es muy importante conocer esta parte desde un punto de vista técnico e histórico.



## DNS Zone Transfer

- Los datos contenidos en una zona DNS son sensibles por naturaleza.
- Individualmente, los registros DNS no son sensibles, pero si un atacante obtiene una copia entera de la zona DNS de un dominio, obtiene una lista completa de todos los Host de ese dominio.
- Un atacante no necesita herramientas especiales para obtener una zona DNS completa, solo que el DNS este mal configurado y que permita a cualquiera realizar una transferencia de zona.
- La transferencia de zona es necesaria y no pueden ser deshabilitadas completamente. Pero solo deben ser permitidas entre servidores DNS y clientes que necesitan de estas.
- En generalmente solo los servidores DNS dependientes necesitan realizar transferencia de zona.

## DNS Denial of Service

- Si un atacante puede realizar una transferencia de zona, también puede realizar ataques de denegación de servicio contra esos servidores DNS realizando múltiples peticiones.



## Whois y ARIN Lookups

- Whois es una herramienta y un protocolo que identifica información de registración de un dominio. Esta definido en el RFC 3912.
- El whois evolucionó desde los primeros Unix hasta los actuales. Las consultas se han realizado tradicionalmente usando una interfaz de línea de comandos, pero actualmente existen multitud de páginas web que permiten realizar estas consultas, aunque siguen dependiendo internamente del protocolo original.
- Utilizando whois, es posible recopilar información de registro como ser el nombre de la persona que realizó el registro del dominio, su correo electrónico, número telefónico y números IP de sus servidores principales.
- Esta información puede atentar contra la privacidad y permitir a los spammers capturar direcciones.



## Whois y ARIN Lookups (Cont.)

- Una URL (uniform resource locator) como www.google.com contiene un nombre de dominio (google.com) y un hostname o alias (www).
- La organización ICANN (Internet Corporation for Assigned Names and Numbers) requiere la registración de dominios para asegurar la unicidad de los mismos. Las herramientas de whois recogen información sobre esta registración oficial obligatoria.

## Whois y ARIN Lookups (Cont.)

- ARIN (American Registry for Internet Numbers) es una organización de registración regional de sitios web.
- Su base de datos incluye información sobre direcciones IP y datos del dueño de un sitio. Puede ser consultada mediante herremientas de whois o en su propio sitio web: http://www.arin.net/whois



## Whois y ARIN Lookups (Cont.)

- Un ethical hacker deberá conocer sobre direcciones IP y sobre como encontrar una ubicación geográfica y camino hacia un objetivo.
- Cada equipo encontrado en la ruta hacia el objetivo puede ser gran fuente de información para futuros procesos.
- Lamentablemente el protocolo whois no está internacionalizado. Un servidor de whois no puede indicar qué codificación de texto usa. Tampoco existe una lista centralizada con todos los servidores whois, por lo que se hace difícil la escritura de herramiententas relacionadas.



## Órganos Autorizados Para Asignación de Números

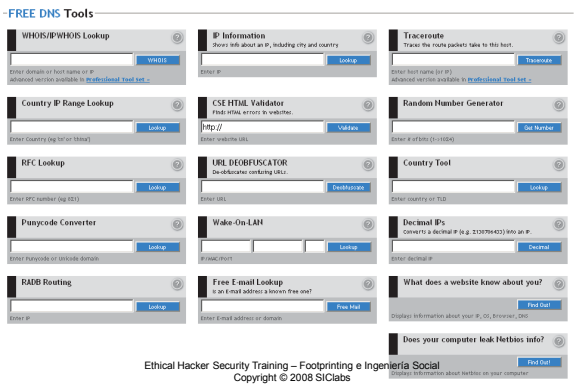
- IANA - Internet Assigned Numbers Authority
  - http://www.iana.com/
- ICANN - Internet Corporation for Assigned Names and Numbers.
  - http://www.icann.org/
- NRO - Number Resource Organisation
  - http://www.nro.net/

## Entidades de Registro por Región Geográfica

- AFRINIC - African Network Information Centre
  - http://www.afrinic.net/
- ARIN - American Registry for Internet Numbers
  - http://ws.arin.net/whois
- LACNIC - Latin America & Caribbean Network Information Centre
  - http://www.lacnic.net/
- RIPE - Réseaux IP Européens Network Coordination Centre
  - http://www.ripe.net/
- APNIC - Asia Pacific Network Information Centre
  - http://www.apnic.net/apnic-bin/whois.pl/

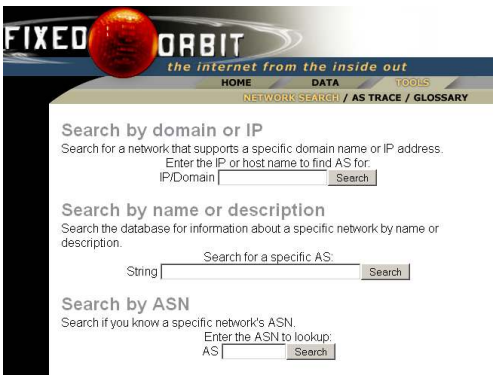


## Herramienta: http://www.dnsstuff.com/






## Herramienta: http://www.fixedorbit.com/

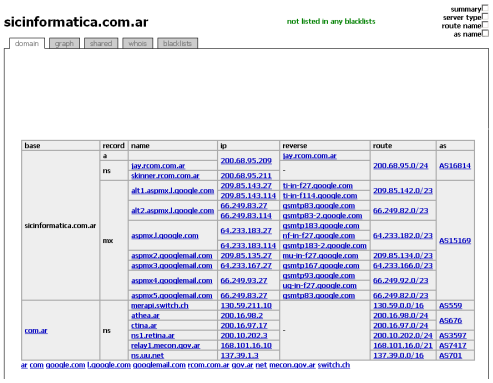


## Herramienta: http://www.traceroute.org/


Ethical Hacker Security Training – Footprinting e Ingeniería Social


## Herramienta: http://www.kartoo.com/


## Herramientas: http://www.robtex.com/




| base | record | name | ip | reverse | route | as |
|---|---|---|---|---|---|---|
| sicinformatica.com.ar | a | | 200.68.95.209 | jay.rcom.com.ar | 200.68.95.0/24 | AS16814 |
| | ns | jay.rcom.com.ar | - | - | | |
| | | skinner.rcom.com.ar | 200.68.95.211 | | | |
| | mx | alt1.aspmx.l.google.com | 209.85.143.27 | ti-in-f27.google.com | 209.85.142.0/23 | AS15169 |
| | | | 209.85.143.114 | ti-in-f114.google.com | | |
| | | alt2.aspmx.l.google.com | 66.249.83.27 | qsmtp83.google.com | 66.249.82.0/23 | |
| | | | 66.249.83.114 | qsmtp83-2.google.com | | |
| | | aspmx.l.google.com | 64.233.183.27 | qsmtp183.google.com | 64.233.182.0/23 | |
| | | | 64.233.183.114 | nf-in-f27.google.com | | |
| | | aspmx2.googlemail.com | 209.85.135.27 | qsmtp183-2.google.com | 209.85.134.0/23 | |
| | | aspmx3.googlemail.com | 64.233.167.27 | mu-in-f27.google.com | 64.233.166.0/23 | |
| | | aspmx4.googlemail.com | 66.249.93.27 | qsmtp167.google.com | 66.249.92.0/23 | |
| | | aspmx5.googlemail.com | 66.249.83.27 | qsmtp93.google.com | 66.249.82.0/23 | |
| | | | | ug-in-f27.google.com | | |
| | | | | qsmtp83.google.com | | |
| com.ar | ns | nerapi.switch.ch | 130.59.211.10 | - | 130.59.0.0/16 | AS559 |
| | | athea.ar | 200.16.98.2 | | 200.16.98.0/24 | AS676 |
| | | ctina.ar | 200.16.97.17 | | 200.16.97.0/24 | |
| | | ns1.retina.ar | 200.10.202.3 | | 200.10.202.0/24 | AS3597 |
| | | relay1.mecon.gov.ar | 168.101.16.10 | | 168.101.16.0/21 | AS7417 |
| | | ns.uu.net | 137.39.1.3 | | 137.39.0.0/16 | AS701 |

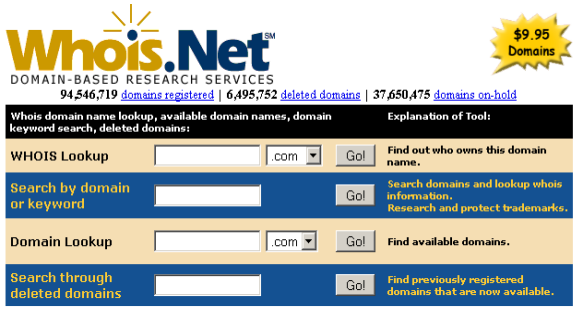
ar com google.com l.google.com googlemail.com rcom.com.ar gov.ar net mecon.gov.ar switch.ch

## Herramientas: http://www.samspade.com/





## Herramientas: http://www.whois.net/







## Herramientas: Firefox Plugins

Shazou


AS Number

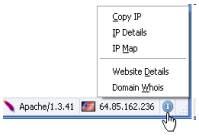
ShowIP


Hostipfox

## Herramientas: Firefox Plugins

DiggiDig

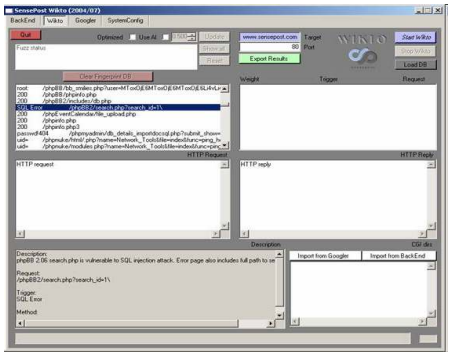
SpiderZilla




Domain Details




## Herramientas: SensePost Wikto



http://www.sensepost.com/research/wikto/

## Identificación de los Tipos de Registros DNS

- **A (address):** Mapea un nombre de host a una dirección IP
- **SOA (Start of Authority):** Define el DNS responsable de la información del dominio.
- **CNAME (canonical name):** Provee nombres adicionales o alias para dicho registro.
- **MX (mail exchange):** Identifica el mailserver del dominio.
- **SRV (service):** Identifica servicios que ofrece el dominio.
- **PTR (pointer):** Mapea direcciones IP a nombres de host

## Identificación de los Tipos de Registros DNS (Cont.)

- **NS (name server):** Identifica otros servidores de nombres para el dominio.
- **HINFO:** Información del host, equipo y sistema operativo
- **TXT:** Información de texto. Permite a los dominios identificarse de modos arbitrarios
- **LOC:** Permite indicar las coordenadas del dominio.
- **WKS:** Generalización del registro MX para indicar los servicios que ofrece el dominio. Está obsoleto en favor de SRV.

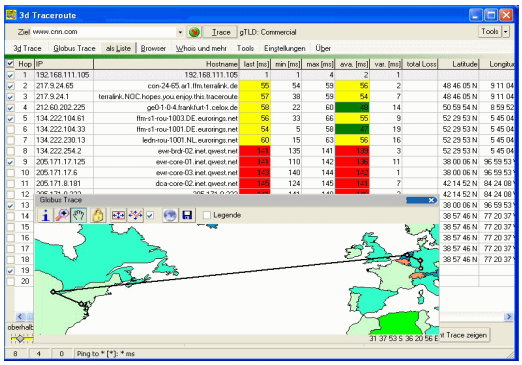


## Traceroute en el Footprinting

- *Traceroute* es una herramienta disponible en todos los S.O. que se utiliza para determinar la ruta de una conexión mediante el envío de un paquete ICMP echo a cada salto (router o gateway) a través del camino hasta el destino.
- Cuando los paquetes son devueltos del router, el TTL (time to live) se decrementa en un punto por cada router a lo largo de la ruta.
- Esto permite determinad cuántos saltos existen desde el origen hasta el destino.
- Uno de los problemas del uso del *traceroute* son los "times out" (indicados con un asterisco). Esto ocurre normalmente al encontrarse un firewall, lo cual también brinda información sobre su existencia y permite luego utilizar técnicas para saltearlo (bypass).
- Las herramientas de *traceroute* visuales pueden ayudar mucho a clarificar las rutas.

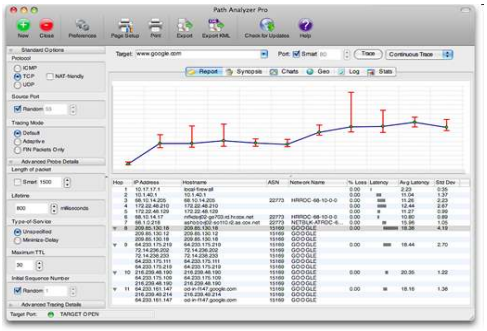


## Herramienta: 3D Traceroute




http://www.d3tr.com/

## Herramienta: Path Analyzer Pro

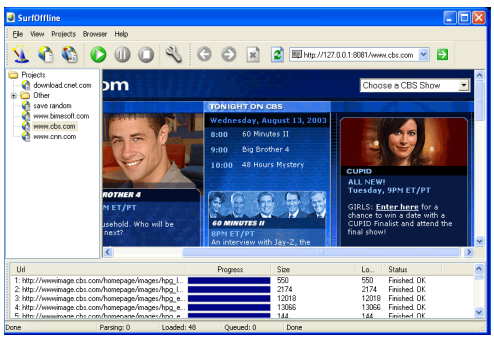


http://www.pathanalyzer.com/

## Herramienta: GEO Spider

http://www.oreware.com

## Herramienta: SurfOffline



http://www.surfoffline.com

## Herramienta: HTTrack


http://www.httrack.com/

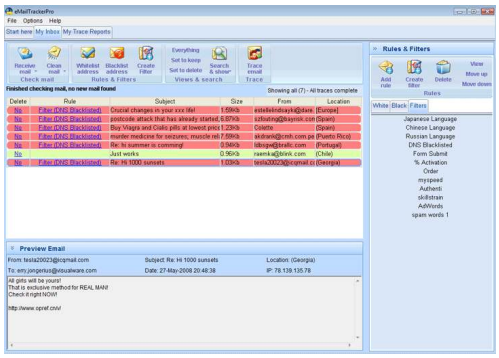
## Herramienta: BlackWidow


http://softbytelabs.com/us/bw/

## E-Mail Tracking

- Los sistemas de “e-mail tracking” permiten saber cuando un destinatario lee, reenvía, modifica o borra un e-mail.
- Muchas aplicaciones de e-mail tracking trabajan agregando un nombre de dominio especial a la dirección de e-mail.
- Luego, un gráfico de un pixel puede notificar las acciones al ser leído dicho pixel.
- Ejemplos:
  - eMailTracking Pro y mailtracking.com

## Herramienta: eMailTrackrPro



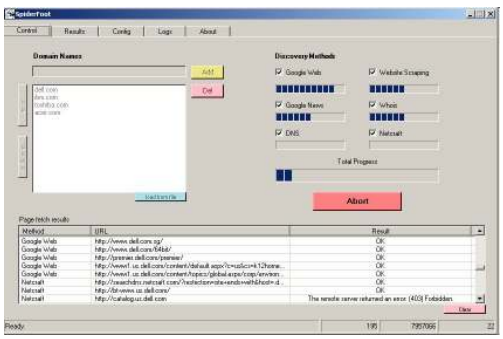
http://www.emailtrackerpro.com

## Web Spiders

- Los spammers y todo interesado en recolectar direcciones de e-mail utilizan web spiders para encontrar direcciones.
- Los web spiders también pueden ser utilizados para encontrar otro tipo de información y pueden automatizar el proceso de reconocimiento.
- Un método para prevenirse del web *spidering* es el uso del archivo "robots.txt" en la raíz del sitio web, indicando la lista de directorios que desea protegerse de la averiguación. Notar que esto también brinda información adicional ;-)

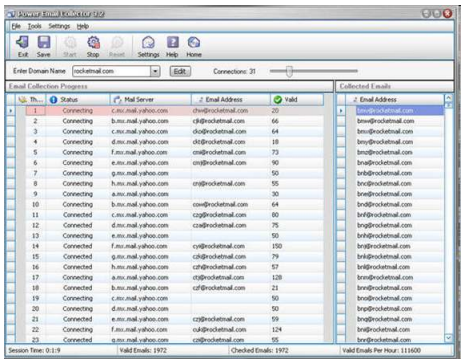



## Herramienta: SpiderFoot



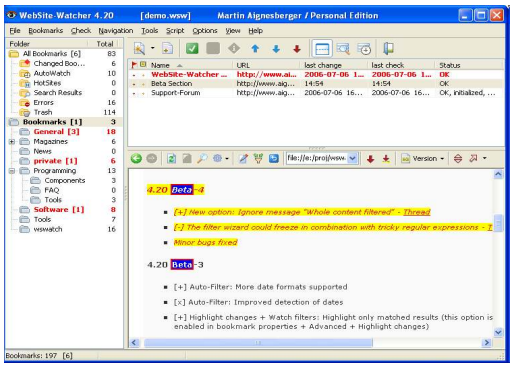
http://www.binarypool.com/spiderfoot/

## Herramienta: Power Email Collector



*http://www.tecsoftware.biz/collector.htm*

## Herramienta: WebSite Watcher



http://www.aignes.com

## ¿Qué es la Ingeniería Social?

- La ingeniería social es un método no técnico para obtener información sobre un sistema, basado en el factor humano, que puede ser utilizada antes o durante un ataque.
- Esto incluye el proceso de engañar a los usuarios, convenciéndolos de que den información que no deberían dar debido a su importancia o sensibilidad.
- La ingeniería social supone el uso de la influencia y persuasión, ya sea personalmente o vía teléfono, e-mail, etc.
- Los métodos tienden a explotar la tendencia natural de las personas a confiar y ayudar a otras personas.
- El uso de estos métodos deja bien claro que el usuario es el eslabón mas débil de la cadena en la seguridad.

## Comportamientos Vulnerables a Ataques

- **Confianza**
  La confianza propia de la naturaleza humana es la base de cualquier ataque de la ingeniería social.
- **Ignorancia**
  La ignorancia o subestimación sobre la ingeniería social y sus efectos hace de la organización un blanco fácil.
- **Miedo**
  Advertencias y amenazas de graves peligros en caso del incumplimiento de la solicitud.
- **Codicia**
  Promesas de algo por nada.
- **Deber moral**
  Cumplimiento de lo solicitado por un sentido de obligación moral.



## Fases de la Ingeniería Social

- Investigación sobre la empresa objetivo
  - Dumpster diving, sitios Web, empleados, visitas a la compañía y más.
- Seleccionar una víctima
  - Identificar empleados frustrados, disconformes, incrédulos, principiantes, etc.
- Desarrollar una relación
  - Desarrollo de una la relación con determinados empleados.
- Explotar las relaciones para alcanzar el objetivo
  - Obtener información sensitiva sobre una cuenta.



## Información Sensible

- Un atacante desea obtener información sensible que de otra forma no podría averiguar, como por ejemplo:
  - Políticas de seguridad
  - Documentos clasificados
  - Infraestructura de red de la oficina
  - Contraseñas

## Tipos de Ataques Comunes

- Podemos dividir la ingeniería social en dos ramas:
  - Human-based: Referida a la interacción de persona a persona, directamente o de manera remota (ej: teléfono).
  - Computer-based: Referida al uso de software para interactuar con el usuario (ej: phishing).
- Una variante mas avanzada es la ingeniería social inversa, que implica que el usuario contacte al atacante sin que este lo solicite.



## Tipos de Ataques Comunes: Human Based

- **Impersonalización**
  Ganar acceso físico simulando ser un usuario válido.
- **El empleado importante**
  Simulación de ser un ejecutivo, gerente, director, etc. que necesita acción inmediata. Se usa la intimidación, ya que nadie cuestionaría a un superior en posición de autoridad.
- **La tercera parte de confianza**
  Suponer la autorización de una tercera persona válida para simular un permiso en realidad inexistente.



## Tipos de Ataques Comunes: Human Based (Cont.)

- **El soporte técnico**
  Simulación de ser personal técnico para la obtención de información.
- **Shoulder surfing**
  Supone la obtención de contraseñas espiando lo que tipea un usuario al autenticarse.
- **Dumpster diving**
  Buscar información escrita o impresiones en la basura.

## Tipos de Ataques Comunes: Computer Based

- Archivos adjuntos en e-mails
- Sitios web falsos
- Ventanas emergentes (popups)



## Tipos de Ataques Comunes: Objetivos Comunes

- Recepcionistas y personal de mesa de ayuda
- Ejecutivos de soporte técnico
- Proveedores de la organización
- Administradores de sistemas y usuarios



## Comprendiendo los Ataques Internos

- Si un hacker no puede averiguar nada sobre una organización, la alternativa será infiltrarse en la misma.
- De esta manera, se podría incluir en una búsqueda laboral o aprovechar algún empleado descontento que quiera colaborar.
- También se puede simular ser un empleado de limpieza, entrega de comida, guardia de seguridad, etc.
- Internamente el acceso a la información es mas directo y libre.
- Se estima que un 60% de los ataques ocurren desde adentro

## Comprendiendo los Ataques Internos (Cont.)

- **Tailgating**
  - Una persona no autorizada, con una credencial de identificación falsa, entra en una zona segura siguiendo de cerca a una persona autorizada que ingresa a través de una puerta que requiere clave de acceso.
  - La persona autorizada desconoce que proporciono a una persona no autorizada el acceso a una zona restringida.
- **Piggybacking**
  - Una persona autorizada proporciona acceso a una persona no autorizada



## Comprendiendo los Ataques Internos (Cont.)

- **Eavesdropping**
  - Escucha de conversaciones o lectura de mensajes de forma no autorizada.
  - Cualquier forma de interceptación, como audio, vídeo o por escrito.



## Comprendiendo los Ataques Internos (Cont.)

- **Contramedidas para las amenazas internas**
  - Separación de las tareas
  - Rotación de las tareas
  - Mínimos privilegios
  - Control de acceso
  - Auditorías y logs
  - Política legal

## Comprendiendo el Robo de Identidad

- Un hacker podría hacer uso del robo de identidad para perpetrar un ataque.
- Las técnicas combinadas de recolección de información podrían permitir la creación de una identificación falsa.
- En organizaciones numerosas habrá mayores controles pero también mayor cantidad de personas, lo cual evita el reconocimiento directo.
- En organizaciones pequeñas, el reconocimiento personal es mas directo, por lo que se ejercen menos controles.



## Ataques de Phishing

- El phishing supone el envío de e-mails, normalmente simulando ser un banco o entidad financiera, en los cuales se requiere confirmación de datos o cualquier razón para justificar el acceso a un sistema online.
- Luego, es probable que la persona se dirija al sitio falso, normalmente mediante el click en un link adjunto.
- Si la persona ingresa sus datos, los estará proporcionando a un entidad falsa creyendo que es real.
- A continuación suele redireccionarse al usuario al sitio real para no levantar sospecha.



## Online Scams

- Algunos sitios web requieren una registración al usuario, y la aprovecha para tomar sus datos de manera real, para luego utilizarlos en otros servicios, dada la alta probabilidad de que se repitan los datos de acceso (usuario y/o password) elegidos.
- Los archivos adjuntos en e-mails pueden ser utilizados para enviar código malicioso de manera sencilla. Este es un tipo de ataque clásico y muy difundido.
- Las ventanas emergentes también pueden utilizarse de manera similar para ofrecer beneficios inexistentes, o sugiriendo la instalación de software malicioso.

## Ofuscación de URLs

- Las URL (Uniform Resource Locator) son utilizadas en la barra de direcciones del navegador para acceder a un sitio en particular.
- La ofuscación de URL implica esconder o falsear la URL real y se utiliza mayormente en ataques de phishing.
- Ejemplo:
  - 200.42.111.56/banco podría parecer una dirección legítima
- La técnica puede incluir el uso de logos reales, pero con hipervínculos falsos, cuya dirección está ofuscada mediante distintas notaciones.
- Ejemplo:
  - La dirección 192.168.10.5 se representa como 3232238085 en decimal o C0A80A05 en hexadecimal



## Contramedidas

- No existe firewall, ni IDS, ni antivirus que proteja contra la ingeniería social dado que no es un ataque técnico.
- Las correctas políticas y procedimientos de seguridad pueden mitigar los ataques de ingeniería social.
- Los programas de concientización (awareness) son sin duda la mejor herramienta para ayudar a evitar que los empleados sean víctimas de este tipo de ataques.



## Footprinting e Ingeniería Social

Referencias y Lecturas Complementarias

## Referencias y Lecturas Complementarias

- **CEH Official Certified Ethical Hacker Review Guide**
  By Kimberly Graves
  (Sybex) ISBN: 0782144373
- **Certified Ethical Hacker Exam Prep**
  By Michael Gregg
  (Que) ISBN: 0789735318
- **Hacking Exposed, Fifth Edition**
  By S.McClure, J.Scambray, and G.Kurtz
  (McGraw-Hill Osborne Media) ISBN: 0072260815
- **Gray Hat Hacking, Second Edition**
  By S.Harris, A.Harper, C.Eagle, J.Ness
  (McGraw-Hill Osborne Media) ISBN: 0071495681




## Footprinting e Ingeniería Social

Preguntas?